

EXHIBIT W:

Claim Chart for the '990 Patent

iControl Inc. "mLOCK"	Patent #: RE 43'990; Independent Claim 125	Patents: 8,106,752; RE 43,990; Dependent Claims
<p>The DHS "TRUST" system Communication Requirements. iControl Inc. locking seal "M-Lock". M-Lock's critical parameter is anti-tamper, multi-modal wireless connectivity. M-Lock's critical function is physical security, location and alerting; and, is available where wireless connectivity is available. 26. A method for autonomous operation of a locking device based on a status of the locking device as recited in claim 23, wherein the one or more sensors include one or more of a movement sensor, a temperature sensor, a humidity sensor, an infrared sensor, a radioactivity detection sensor, an acoustic sensor, and a chemical detection sensor. (Patent application: mLOCK Device and Associated Methods; US 20100283575 A1)</p>	<p>A multi-sensor detection system for monitoring products and capable of operating with at least one of a designated perimeter sensor, a range sensor, a human sensor, a light sensor, a video sensor, a tampering sensor, a breach sensor, a temperature sensor, or a door sensor for an unauthorized or unscheduled door opening, comprising:</p>	<p>148. The multi sensor detection security systems [of claim 145], further including at least one sensor of system failure, motion, infrared, perimeter, temperature, tampering or breach, for the prevention of terrorist activity and theft.</p>

<p>A user may connect a computing device, such as a handheld computing device or laptop computer, to the data interface 123 to communicate with the LDD 111 or processor 103. A current proximity of the locking device to a wireless communication network to which the computing system can wirelessly communicate.</p>	<p>at least one communication device of a cell phone, a cell phone detector case, a smart phone, a handheld, a PDA, a laptop, or a computer terminal at a monitoring site, and wherein the communication device has a central processing unit (cpu);</p>	<p>135. The multi-sensor detection system [of claim 125] wherein the internal or external remote/electrical lock disabler is designed to be equipped with applications for the locking, disabling a lock, enabling a lock, and unlocking the locks of, but not limited to, containers, vehicles, houses and businesses, using a smart phone, cell phone, PDA, laptop or desktop.</p>
<p>A current proximity of the locking device to a wireless communication network to which the computing system can wirelessly communicate, a temperature near the locking device, a humidity near the locking device, a radioactivity level near the locking device, a chemical presence near the locking device, and an external movement near the locking device.</p>	<p>at least one sensor that is a designated perimeter sensor, range sensor, human sensor, light sensor, video sensor, tampering sensor, breach sensor, temperature sensor, or door sensor for unauthorized or unscheduled door opening, interconnected to the at least one communication device for communication therebetween;</p>	<p>35. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device is designed to unlock or enable the lock of the product thus allowing access to the product by authorized, trained, and equipped individuals.</p>

<p>Upon arrival at the airport, a TSA agent looks at the mLOCK 100 user interface display 144 to see if an alarm was generated in route. If so, the mLOCK 100 is removed and the truck is inspected. If not, the mLOCK 100 is removed and returned to the freight forwarder for use in future shipments. [W]herein some of the one or more sensors proximate to the locking device are physically attached to the locking device and communicate data with the computing system through wired connections.</p>	<p>wherein the at least one interchangeable sensor is interconnected to an internal or external remote/electrical lock disabler;</p>	<p>36. The automatic/mechanical lock disabler system [of claim 35] wherein the automatic/mechanical lock disabler [of claim 35] includes a plurality of interchangeable and integrable sensors for detecting the chemical, biological, radiological, nuclear, explosive and contraband agents and compounds to include sensors for detecting humans, motion, temperature, shock and tampering which is capable of being disposed within the detector case. Patent 8,106,752</p>
<p>3. A locking device as recited in claim 2, further comprising: a solar film electrically connected to the power source and defined to electrically recharge the power source. 4. A locking device as recited in claim 1, wherein the radio is an international frequency radio, and wherein the location determination device is a global positioning system receiver device.</p>	<p>at least one of an Internet connection, a GPS connection, or a power connection disposed within the internal or external remote/electrical lock disabler;</p>	<p>39. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device has a power connection which is interconnected to the central processing unit (cpu) and includes a power source of battery, electrical or solar.</p>

<p>The mLOCK 100 is an electronic lock that secures an asset, such as cargo within a shipping container, by controlling the ability to operate a locking mechanism of the mLOCK 100 based on proximity to secure networks, geographic locations, or via user commands through a radio link. Based on the automatically determined real-time status of the locking device, operating the computing system to automatically control a locking mechanism of the locking device to either lock or unlock the locking device. The locking mechanism of the mLOCK 100 is secured through a mechanical mechanism that inhibits opening a shackle of the mLOCK 100 unless an electro-mechanical lock actuator 146 enables such operation of the mLOCK 100.</p>	<p>wherein the internal or external remote/electrical lock disabler communicates with the communication device and the internal or external remote/electrical lock disabler is mounted, embedded, affixed, or attached to a product for receiving transmission from the communication device to lock or disable a lock on the product and to prevent access to the product by unauthorized, untrained, and unequipped individuals, wherein the internal or external automatic/mechanical lock disabler detection device engages the lock on the product; and</p>	<p>35. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device is designed to unlock or enable the lock of the product thus allowing access to the product by authorized, trained, and equipped individuals.</p>
--	--	---

<p>17. A method for autonomous operation of a locking device based on a status of the locking device, comprising: operating a computing system onboard the locking device to automatically determine a real-time status of the locking device. The data signal may be a push button signal, an intrusion alarm signal, a chemical/biological agent detection signal, a temperature signal, a humidity signal, or essentially any other type of signal that may be generated by a sensing device.</p>	<p>whereupon detection causes a signal to be sent to the at least one communication device followed by communicating with the internal or external remote/electrical lock disabler.</p>	<p>44. The lock disabler system [of claim 33] wherein the automatic/mechanical lock disabler detection device can send and receive signals, send and receive warnings, send and receive commands, send and receive data, information and report the status of the sensors and operational equipment systems to a cell phone, smart phone, PDA or handheld device.</p>
--	---	---